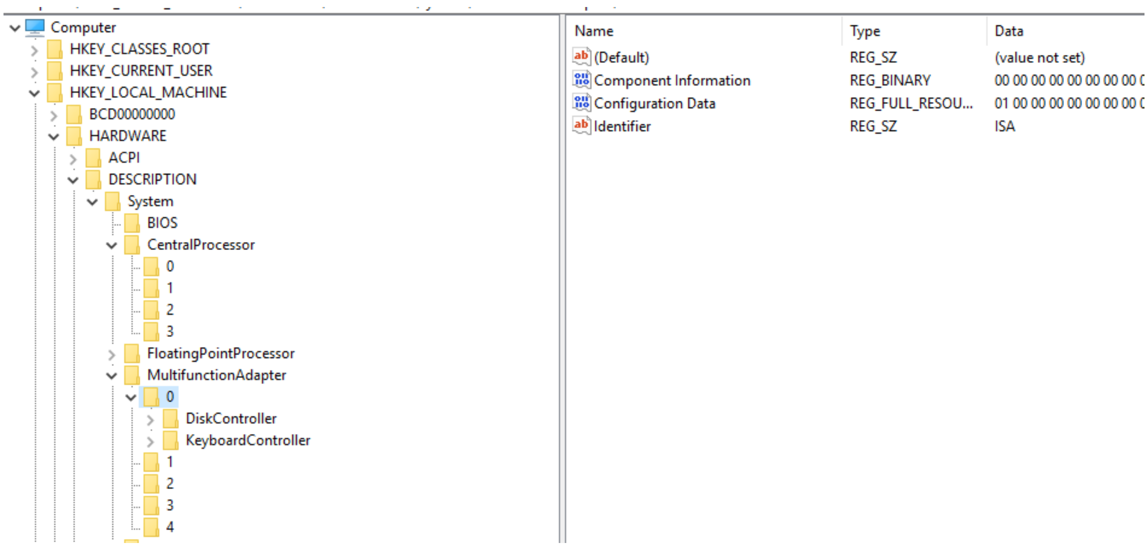
Digging Through Registry Keys, Recursively & Remotely with PowerShell

Summary

A common scenario that I encounter is having to dig through registry hives on remote Windows workstations to programmatically collect information. This poses an interesting challenge because sometimes there is an unknown quantity of elements contained within a registry key; the names of the values contained within a key, and the names & quantities of each [sub-]key's sub-keys. In the screenshot below, the 'Hardware' key contains multiple sub-keys. Some of these sub-keys contains contain values and additional nested sub-keys.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Component Information	REG_BINARY	00 00 00 00 00 00 00 00 (
Configuration Data	REG_FULL_RESOU...	01 00 00 00 00 00 00 00 (
Identifier	REG_SZ	ISA

Figure 1

Because the sub-keys' depth, and value names are unknown, we need a special type of function that can handle these unknowns quantities & depths. To solve this problem, we use what is known as a 'recursive' function, which is a function that contains code that calls that same function again. For example, in this snippet of code, the function someRecursiveFunction accepts a parameter named $value. Within the function, an if statement evaluates a condition. If the condition returns TRUE, the function is called again.

```
Function someRecursiveFunction($value)
{
        If(condition)
        {
                #recursion…
                someRecursiveFunction -value $value
        }
}
```

Our registry-key-digging recursive function will go around-and-around, digging through and unknown number of registry sub-keys, each having an unknown depth. The functionality & logic are simple, but it can be initially a bit confusing to visualize. The first thing that our function will do is open the initial key, or starting point, and check to see if it contains sub-keys. If it contains sub-keys, it proceeds to retrieve all the sub-key's value names & values (if there are any), and then it passes each sub-key into the same function. Again, the function checks for the presence of sub-keys, retrieve values, and so on, until all sub-keys & values have been evaluated. When it encounters a key that does not contain any sub-keys, it retrieves the values from that particular key, and continues. If any of the keys, and/or sub-keys do not contain any values, it advances to the next element.

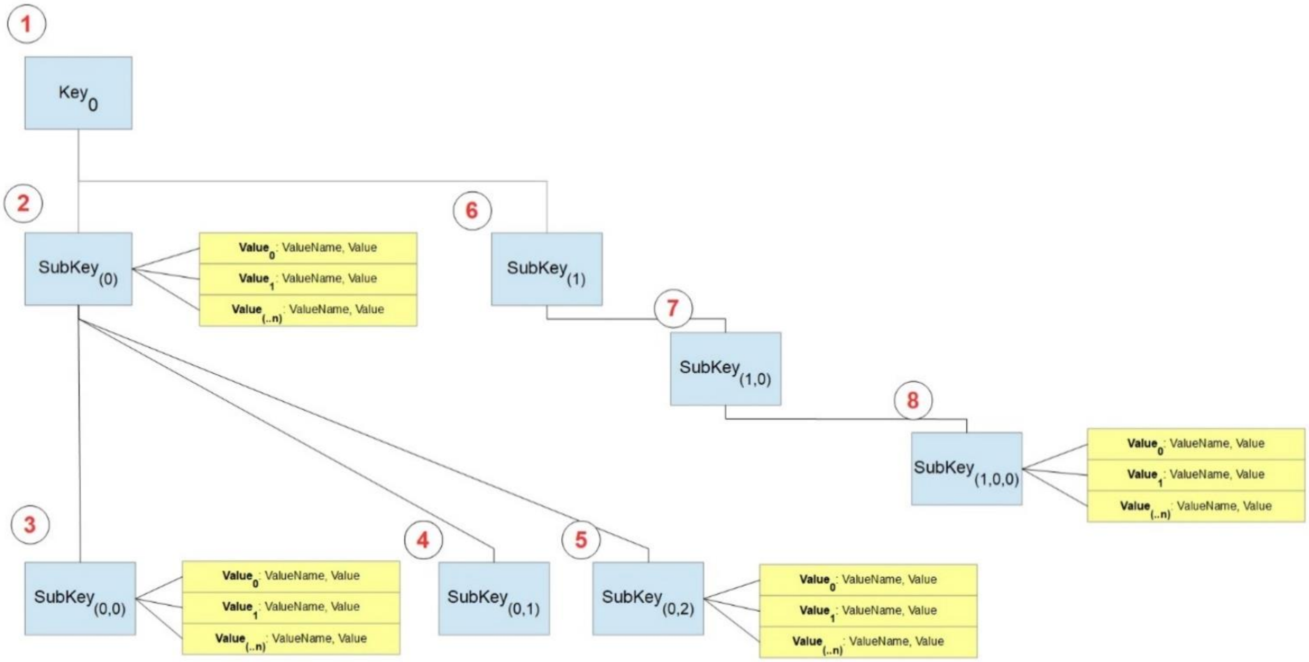
Process

1. Open Key
    1. Does it contain sub-keys?
        - A. Yes
            1. Get Values in **Key**. Add values to array.
            2. For-Each **sub-key**, send **sub-key** to step #1
        - B. No
            1. Get Values in **Key**. Add values to array.

Example Scenario

In the scenario illustrated below (Figure 2.), the order of operations is as follows:

2. Open Key$_0$
3. Get values from SubKey$_0$.
4. Get Values from SubKey$_{0,0}$
5. Get values from SubKey$_{0,1}$
6. Get values from SubKey$_{0,2}$
7. Get values from SubKey$_1$
8. Get values from SubKey$_{1,0}$
9. Get values form SubKey$_{1,0,0}$



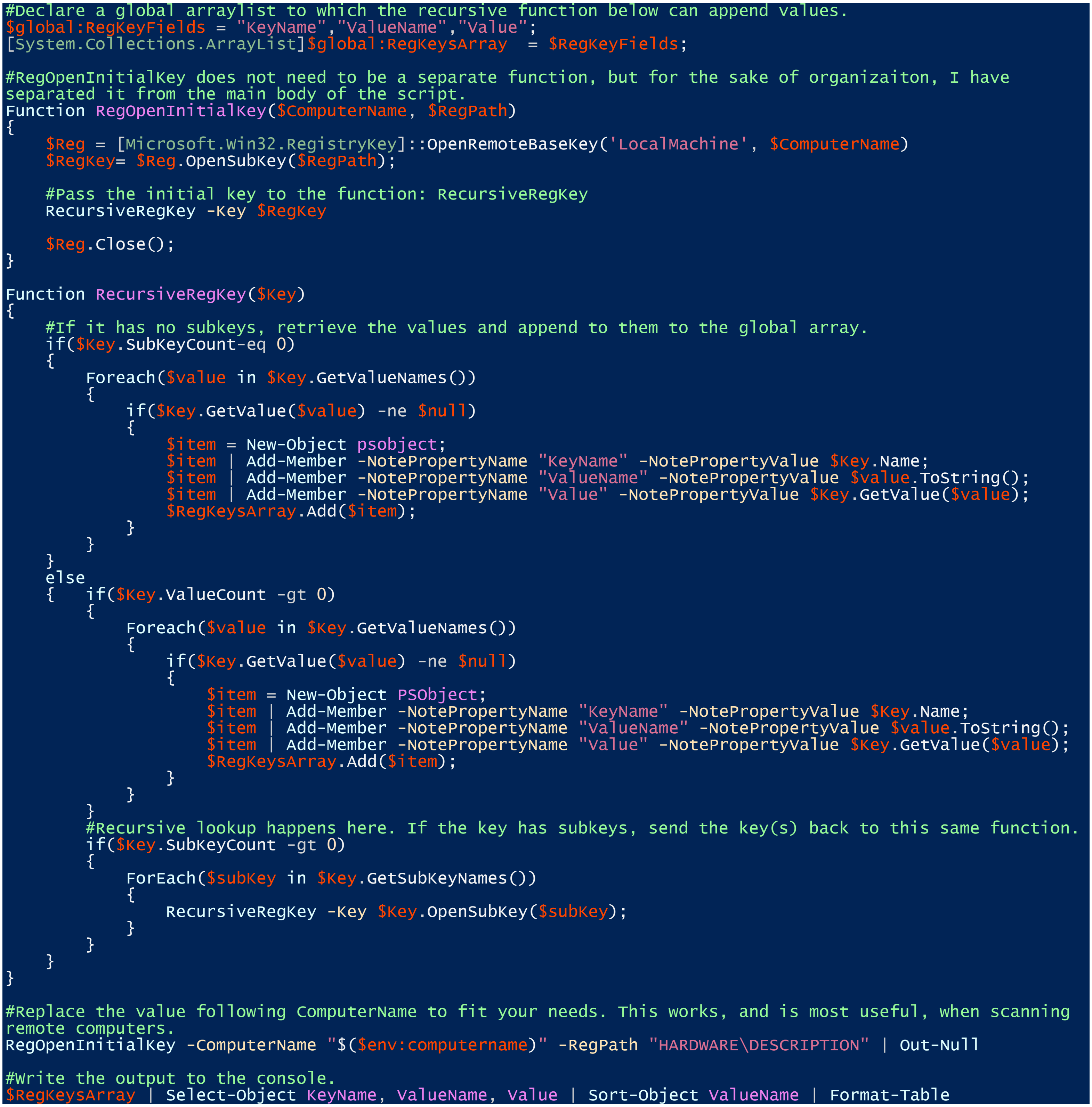
1
Key$_0$
2
SubKey$_{(0)}$
Value$_0$: ValueName, Value
Value$_1$: ValueName, Value
Value$_{(..n)}$: ValueName, Value
6
SubKey$_{(1)}$
7
SubKey$_{(1,0)}$
8
SubKey$_{(1,0,0)}$
Value$_0$: ValueName, Value
Value$_1$: ValueName, Value
Value$_{(..n)}$: ValueName, Value
3
SubKey$_{(0,0)}$
Value$_0$: ValueName, Value
Value$_1$: ValueName, Value
Value$_{(..n)}$: ValueName, Value
4
SubKey$_{(0,1)}$
5
SubKey$_{(0,2)}$
Value$_0$: ValueName, Value
Value$_1$: ValueName, Value
Value$_{(..n)}$: ValueName, Value

Figure 2.

PowerShell Script

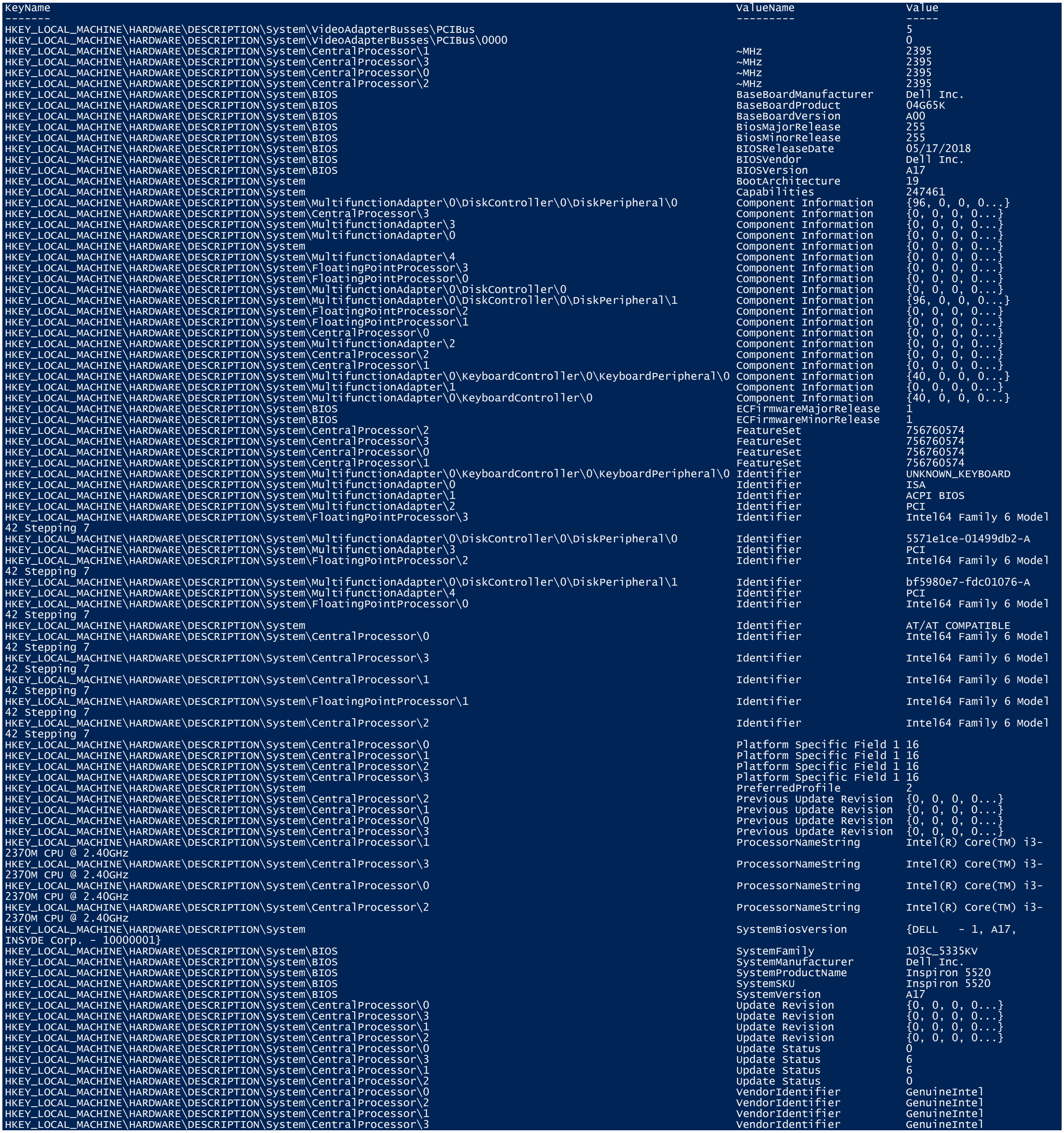
The script below opens HKEY Local Machine, and recursively probes all the **Hardware\Description** key's values, along with all of its sub-keys and their values. These values are stored in an array list. When the scan has completed, the array is sorted, and output is sent to the console as a table.

To modify this code to probe a different key, change the initial *RegPath* value when calling the **RegOpenInitialKey** function. It is currently set to, "HARDWARE\DESCRIPTION". To probe a remote machine, change the ComputerName value to the name of the remote computer that you wish to scan.



```powershell
#Declare a global arraylist to which the recursive function below can append values.
$global:RegKeyFields = "KeyName","ValueName","Value";
[System.Collections.ArrayList]$global:RegKeysArray  = $RegKeyFields;

#RegOpenInitialKey does not need to be a separate function, but for the sake of organizaiton, I have
separated it from the main body of the script.
Function RegOpenInitialKey($ComputerName, $RegPath)
{
    $Reg = [Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey('LocalMachine', $ComputerName)
    $RegKey= $Reg.OpenSubKey($RegPath);

    #Pass the initial key to the function: RecursiveRegKey
    RecursiveRegKey -Key $RegKey

    $Reg.Close();
}

Function RecursiveRegKey($Key)
{
    #If it has no subkeys, retrieve the values and append to them to the global array.
    if($Key.SubKeyCount-eq 0)
    {
        Foreach($value in $Key.GetValueNames())
        {
            if($Key.GetValue($value) -ne $null)
            {
                $item = New-Object psobject;
                $item | Add-Member -NotePropertyName "KeyName" -NotePropertyValue $Key.Name;
                $item | Add-Member -NotePropertyName "ValueName" -NotePropertyValue $value.ToString();
                $item | Add-Member -NotePropertyName "Value" -NotePropertyValue $Key.GetValue($value);
                $RegKeysArray.Add($item);
            }
        }
    }
    else
    {   if($Key.ValueCount -gt 0)
        {
            Foreach($value in $Key.GetValueNames())
            {
                if($Key.GetValue($value) -ne $null)
                {
                    $item = New-Object PSObject;
                    $item | Add-Member -NotePropertyName "KeyName" -NotePropertyValue $Key.Name;
                    $item | Add-Member -NotePropertyName "ValueName" -NotePropertyValue $value.ToString();
                    $item | Add-Member -NotePropertyName "Value" -NotePropertyValue $Key.GetValue($value);
                    $RegKeysArray.Add($item);
                }
            }
        }
        #Recursive lookup happens here. If the key has subkeys, send the key(s) back to this same function.
        if($Key.SubKeyCount -gt 0)
        {
            ForEach($subKey in $Key.GetSubKeyNames())
            {
                RecursiveRegKey -Key $Key.OpenSubKey($subKey);
            }
        }
    }
}

#Replace the value following ComputerName to fit your needs. This works, and is most useful, when scanning
remote computers.
RegOpenInitialKey -ComputerName "$($env:computername)" -RegPath "HARDWARE\DESCRIPTION" | Out-Null

#Write the output to the console.
$RegKeysArray | Select-Object KeyName, ValueName, Value | Sort-Object ValueName | Format-Table
```

Console Output



```
KeyName                                                                                                         ValueName                 Value
-------                                                                                                         ---------                 -----
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\VideoAdapterBusses\PCIBus                                                                  5
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\VideoAdapterBusses\PCIBus\0000                                                             0
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1                                               ~MHz                      2395
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3                                               ~MHz                      2395
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0                                               ~MHz                      2395
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2                                               ~MHz                      2395
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             BaseBoardManufacturer     Dell Inc.
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             BaseBoardProduct          04G65K
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             BaseBoardVersion          A00
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             BiosMajorRelease          255
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             BiosMinorRelease          255
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             BIOSReleaseDate           05/17/2018
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             BIOSVendor                Dell Inc.
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             BIOSVersion               A17
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System                                                                  BootArchitecture          19
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System                                                                  Capabilities              247461
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0\DiskController\0\DiskPeripheral\0         Component Information     {96, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3                                               Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\3                                           Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0                                           Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System                                                                  Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\4                                           Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\FloatingPointProcessor\3                                         Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\FloatingPointProcessor\0                                         Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0\DiskController\0                          Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0\DiskController\0\DiskPeripheral\1         Component Information     {96, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\FloatingPointProcessor\2                                         Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\FloatingPointProcessor\1                                         Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0                                               Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\2                                           Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2                                               Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1                                               Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0\KeyboardController\0\KeyboardPeripheral\0 Component Information     {40, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\1                                           Component Information     {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0\KeyboardController\0                      Component Information     {40, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             ECFirmwareMajorRelease    1
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             ECFirmwareMinorRelease    1
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2                                               FeatureSet                756760574
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3                                               FeatureSet                756760574
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0                                               FeatureSet                756760574
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1                                               FeatureSet                756760574
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0\KeyboardController\0\KeyboardPeripheral\0 Identifier                UNKNOWN_KEYBOARD
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0                                           Identifier                ISA
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\1                                           Identifier                ACPI BIOS
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\2                                           Identifier                PCI
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\FloatingPointProcessor\3                                         Identifier                Intel64 Family 6 Model
42 Stepping 7
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0\DiskController\0\DiskPeripheral\0         Identifier                5571e1ce-01499db2-A
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\3                                           Identifier                PCI
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\FloatingPointProcessor\2                                         Identifier                Intel64 Family 6 Model
42 Stepping 7
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0\DiskController\0\DiskPeripheral\1         Identifier                bf5980e7-fdc01076-A
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\4                                           Identifier                PCI
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\FloatingPointProcessor\0                                         Identifier                Intel64 Family 6 Model
42 Stepping 7
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System                                                                  Identifier                AT/AT COMPATIBLE
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0                                               Identifier                Intel64 Family 6 Model
42 Stepping 7
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3                                               Identifier                Intel64 Family 6 Model
42 Stepping 7
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1                                               Identifier                Intel64 Family 6 Model
42 Stepping 7
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\FloatingPointProcessor\1                                         Identifier                Intel64 Family 6 Model
42 Stepping 7
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2                                               Identifier                Intel64 Family 6 Model
42 Stepping 7
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0                                               Platform Specific Field 1 16
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1                                               Platform Specific Field 1 16
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2                                               Platform Specific Field 1 16
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3                                               Platform Specific Field 1 16
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System                                                                  PreferredProfile          2
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2                                               Previous Update Revision  {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1                                               Previous Update Revision  {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0                                               Previous Update Revision  {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3                                               Previous Update Revision  {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1                                               ProcessorNameString       Intel(R) Core(TM) i3-
2370M CPU @ 2.40GHz
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3                                               ProcessorNameString       Intel(R) Core(TM) i3-
2370M CPU @ 2.40GHz
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0                                               ProcessorNameString       Intel(R) Core(TM) i3-
2370M CPU @ 2.40GHz
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2                                               ProcessorNameString       Intel(R) Core(TM) i3-
2370M CPU @ 2.40GHz
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System                                                                  SystemBiosVersion         {DELL   - 1, A17,
INSYDE Corp. - 10000001}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             SystemFamily              103C_5335KV
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             SystemManufacturer        Dell Inc.
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             SystemProductName         Inspiron 5520
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             SystemSKU                 Inspiron 5520
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS                                                             SystemVersion             A17
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0                                               Update Revision           {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3                                               Update Revision           {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1                                               Update Revision           {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2                                               Update Revision           {0, 0, 0, 0...}
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0                                               Update Status             0
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3                                               Update Status             6
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1                                               Update Status             6
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2                                               Update Status             0
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0                                               VendorIdentifier          GenuineIntel
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2                                               VendorIdentifier          GenuineIntel
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1                                               VendorIdentifier          GenuineIntel
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3                                               VendorIdentifier          GenuineIntel
```